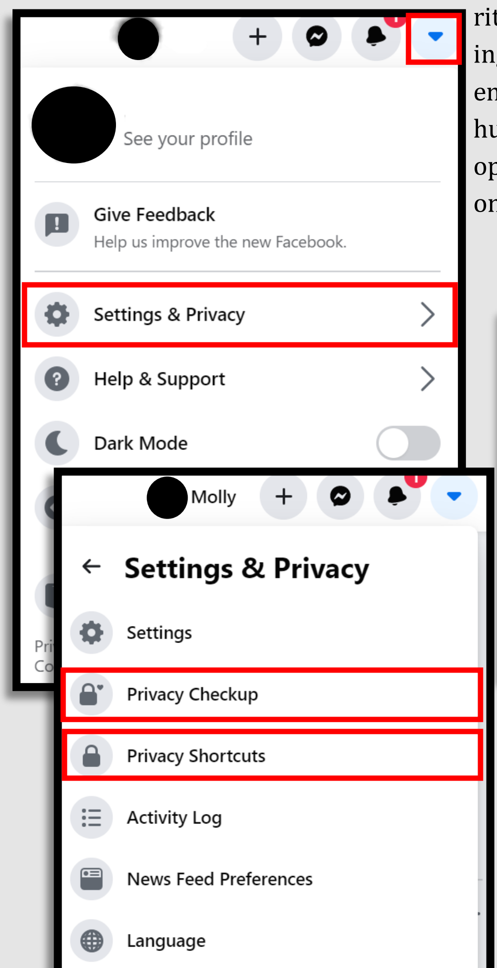
FACEBOOK SMART CARD

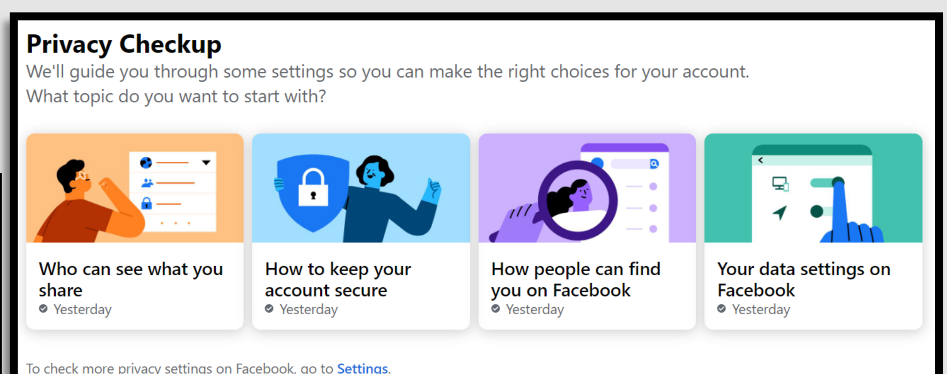
Do's and Don'ts

- Do use pictures of something other than yourself for cover and profile photos. Cover and profile photos are viewable to the "Public". Remember if you change your profile picture you must change the privacy setting from "Public" to perhaps "Friends", Facebook will not do it for you.
- Do use caution when posting images and videos of you or your family. Be aware of your surroundings, to include identifiable locations and any other personal security vulnerabilities.
- Do select "Only Me" or "Friends" for all available settings options. Ensure that family members take similar precautions with their accounts. Their privacy and share settings can expose your personal data.
- Don't add your birthdate, location, phone number, or other personal details to your profile. If you do add this information make sure you set it so that it is not "Public".
- Don't link your Facebook account to any third party applications such as Twitter, LinkedIn, or gaming apps.
- Don't establish connections with individuals you do not know and trust. Understand that not everyone is who they say they are.
- Don't discuss specific details online, keep discussions general. When posting pictures, ensure that no personal information can be seen in the background. For instance, if you are posting a picture of your car you will want to make sure the license plate is not showing.

New Design & Quick Privacy

Facebook published a new platform design in 2020, with the purposes of providing a simplified user experience closer to the mobile app version, faster performance, and new features. Facebook's new design provides several privacy and security updates, most notably more access to information and explanations regarding your options. The information provided in these pages will walk through the entire process of locking down your Facebook account. However, if you are in a hurry, you can access an abbreviated version of Facebook's privacy and security options by going through the "Privacy Checkup" and "Privacy Settings" features on your account. Start at your "Home Page", select the "Down Arrow" in the top



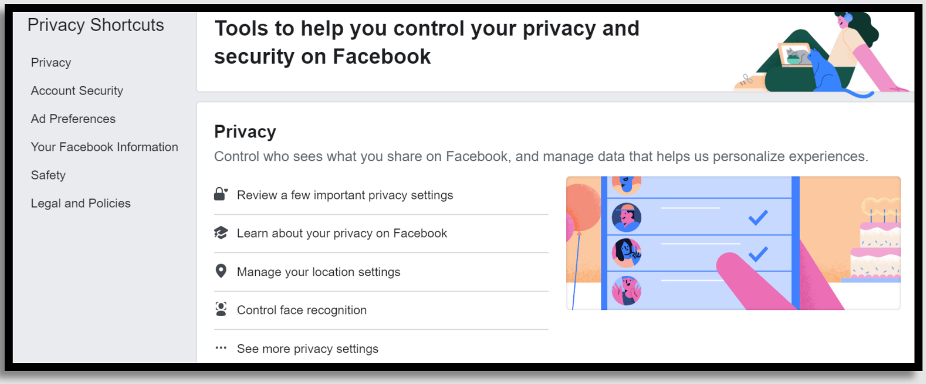


Next, select "Privacy Checkup", and walk through each box on the screen that follows. Again, it is an abbreviated version of the manual provided here, we recommend you work though this whole Card at your convenience. You could also use this feature to complete easy quick checks on a regular basis, for instance each month, just to make sure you stay on top of changes.

Facebook quizzes could be taking more from you than you realize, Think twice about finding out which Star Wars character you are. #keepyouridentitysafe

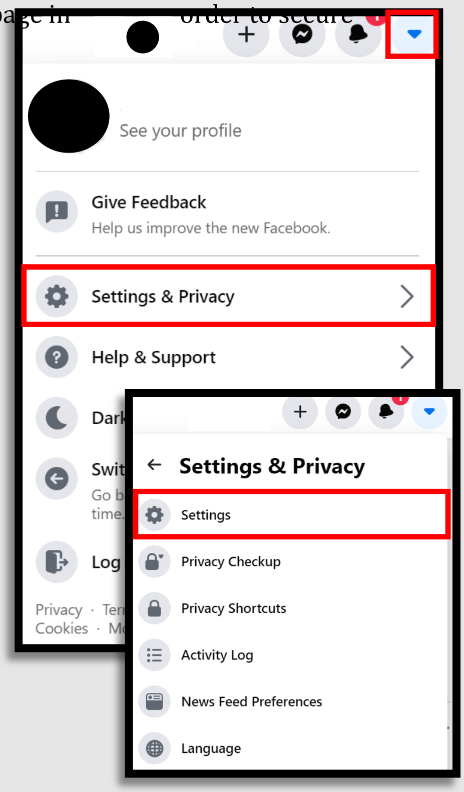
FACEBOOK SMART CARD

Personal Computer (PC) Version



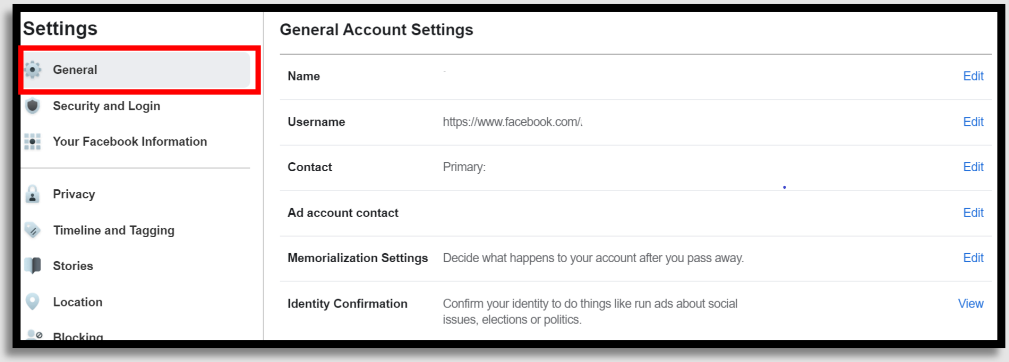
Secondly, you can select "Privacy Shortcuts" (see previous page), which will take you to the page seen here to the right. Here, you can go through some additional privacy information (all of which will be covered in the coming pages), and access useful information about things like privacy, how Facebook's ad policy and processes work, and resources for parents. Again, feel free to go through this information, but also complete the full Card, beginning below, for our most thorough lock down guidance.

Facebook continuously works to enhance its privacy efforts and better protect user data. As a result, many settings have changed and more have been added. To begin, click the "Down Arrow" at the top right corner of the Facebook screen. From the drop down, select "Settings and Privacy", and then "Settings". You will want to go through each menu item on the next page in order to secure



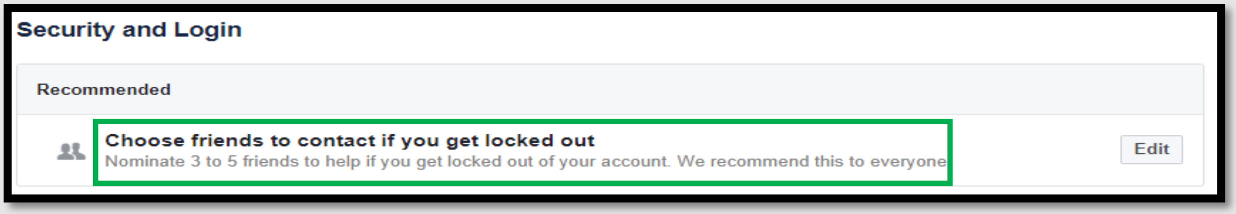
General Account Settings

Starting in the "General" section (see below), go through and review your information. Remember, your "Username" (which is located in the URL) will be "Public" on Facebook, just as your "Name" is. In this section you can add a new email address and phone number, direct what happens with your account when you die, and direct Facebook ads to a new email address.



Friends can help if you get locked out!

Next, head back to the left-hand column and select "Security and Login". Here you can check and update your security settings and see all the places that Facebook thinks you are logged in at. First look at the "Recommended" section, shown below. It is recommended that you choose friends that can help you to log in to Facebook should you ever become locked out.



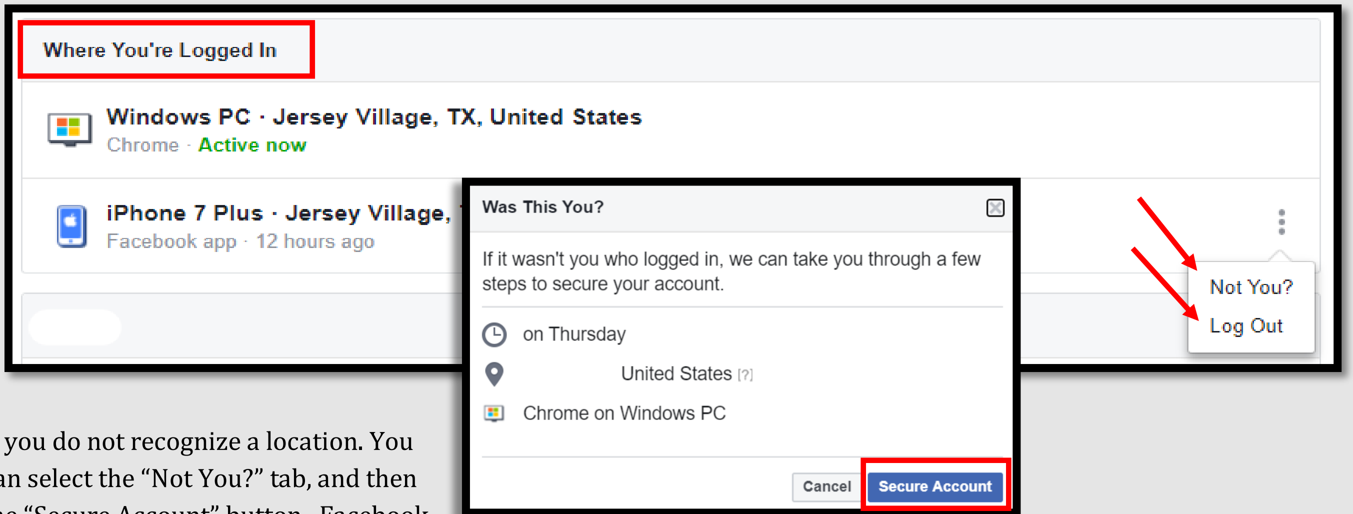
It is not possible to lock down someone else's account so it is important to note the privacy setting on a post before you "Comment" or "React" to each post. #privacymatters

FACEBOOK SMART CARD

Personal Computer (PC) Version

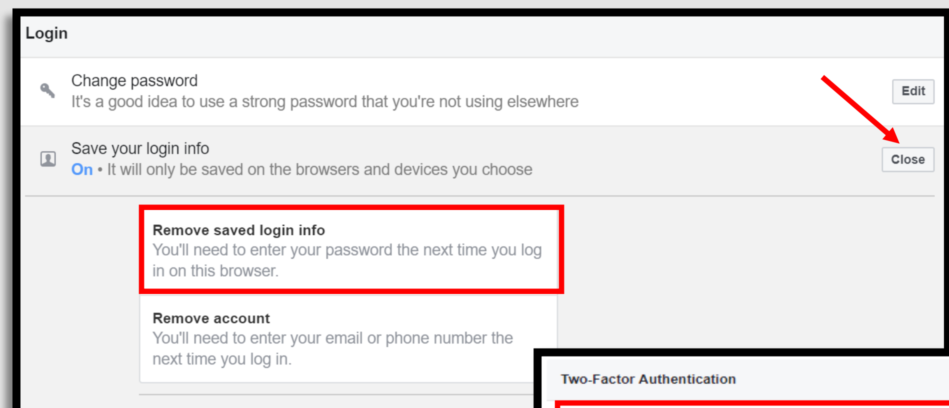
Login & Two Factor Authentication

Once you have selected your friends as an additional security measure, scroll to the "Where You're Logged in at" box and look to ensure you recognize each location Facebook says you are logged in from. Some of these locations can be repetitive based on how many times you log in or for each different session.



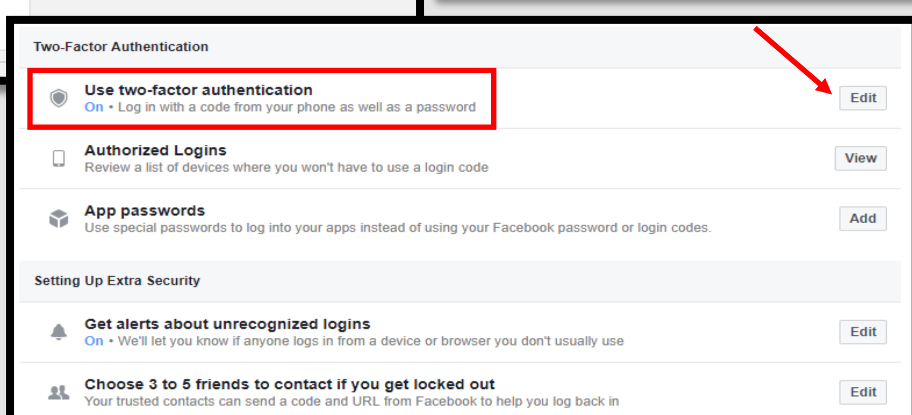
If you do not recognize a location. You can select the "Not You?" tab, and then the "Secure Account" button. Facebook will take you through some steps to help you ensure your account is secure.

Next, under "Login", and "Save your login info", you have the choice to keep yourself logged in on any device you choose. We recommend that you NOT enable this function, and instead choose to log in each time you open Facebook. This way your account is secure even if you lose your computer or mobile device. Select the "Edit" button to the right, and then select "Remove saved login info".



An unrecognized login location can be the result of a few different things. First, when signing in via mobile device, you may be routed through an IP address that doesn't reflect your actual location. Second, Facebook may have inaccurate information. Third, you may remain logged into a device that you logged onto in an alternate location. And finally someone else could have unauthorized access to your Facebook account. If an unrecognized location seems to be due to unauthorized access it is recommended that you immediately go in and change your password on both Facebook and your email account.

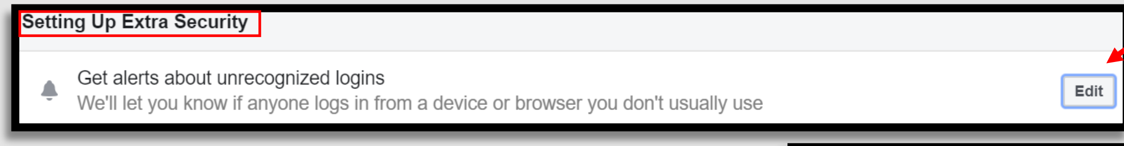
We recommend that you enable "Two-factor Authentication" in order to equip your account with the highest level of security available. Click on the "Edit" button to the right of "Use two-factor authentication", and choose the security method you prefer or are most familiar with. A security code will be sent to you for entry each time you log in.

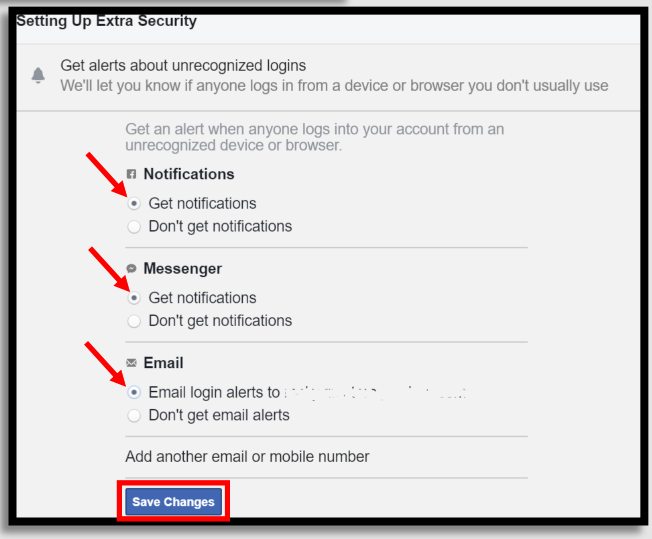


It is not possible to lock down someone else's account so it is important to note the privacy setting on a post before you "Comment" or "React" to each post. #privacymatters

FACEBOOK SMART CARD

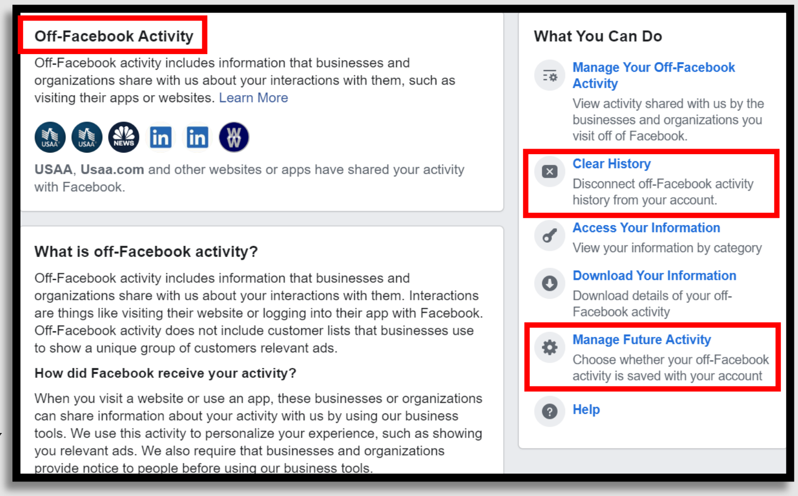
Personal Computer (PC) Version



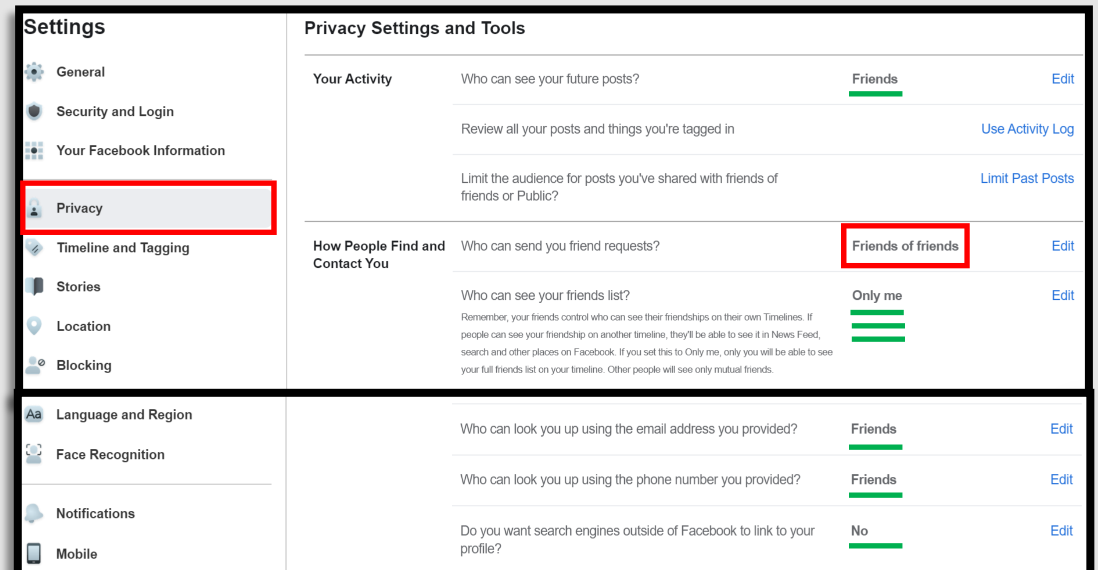


Finally, it is a good idea to request notification in the case that someone logs into your account without your permission. To do this, under "Setting Up Extra Security", and "Get alerts about unrecognized logins", to the right, click the "Edit" button. Then select the buttons under "Facebook Notification", "Messenger" and/or "Email" to direct where you would like to receive such messages. To complete, click on the "Save Changes" button.

Next, go back to the column on the left hand side and select "Your Facebook information". Here you can easily manage the information you have allowed onto Facebook or delete your account entirely. * Time Saver...both the "Access Your Information" and "Activity Log" sections take you to the same "Activity Log" page, and allow you to manage your information.



Next select "Off-Facebook Activity" and clear your history. It is highly recommended that you forbid Facebook from tracking your "Offline Activity. Select "Clear History" and click on the "Clear History" button on the pop-up. Also consider selecting "More Options", then "Manage Future Activity" in order to limit the kinds of information Facebook can collect from your "Off-Facebook Activity " in the future. Follow the prompts to "Manage Future Activity".



Now look at the tabs on the left and find the "Privacy" section. Completing this section is one of the most important aspects to keeping your information safeguarded on Facebook. This section puts you, the user, in charge of decisions about where your data goes and who can see it. Take some time here to ensure each section is set to your preference. *** Guidance for the image to the left "Privacy Settings and Tools" page is found on the following page. ***

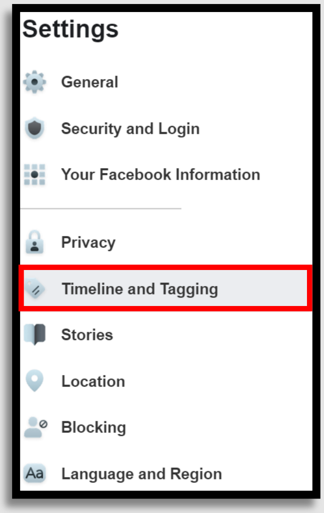
Never become complacent with your Privacy settings. Checking your settings once a quarter could help to keep your information safe online. #updatethoseprivacysettings

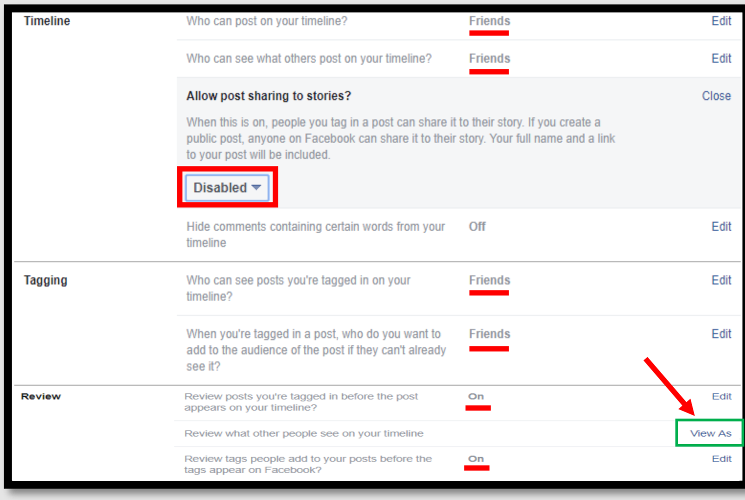
FACEBOOK SMART CARD

Personal Computer (PC) Version

*** This paragraph applies to the "Privacy Settings & Tools" page image above, or on the previous page. *** We recommend no category be set to "Public". Preferable settings are noted below. We recommend choosing "Only Me" wherever possible, but understand that this sometimes undermines the social purpose of Facebook. Still, we strongly recommend you leave the "Only Me" setting for "Who can see your friends list" in order to protect yourself and your social network—this list simply gives away too much information about you. Where you cannot leave "Only Me", the next best option is to choose "Friends". Finally, we recommend you do NOT allow Facebook to link other search engines to your profile.

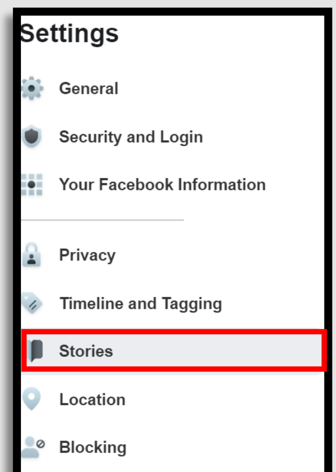
Privacy & Stories



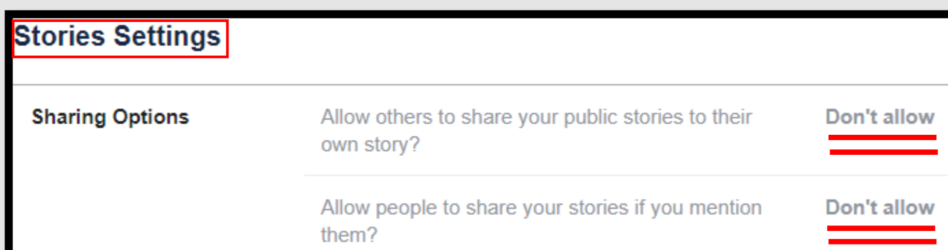


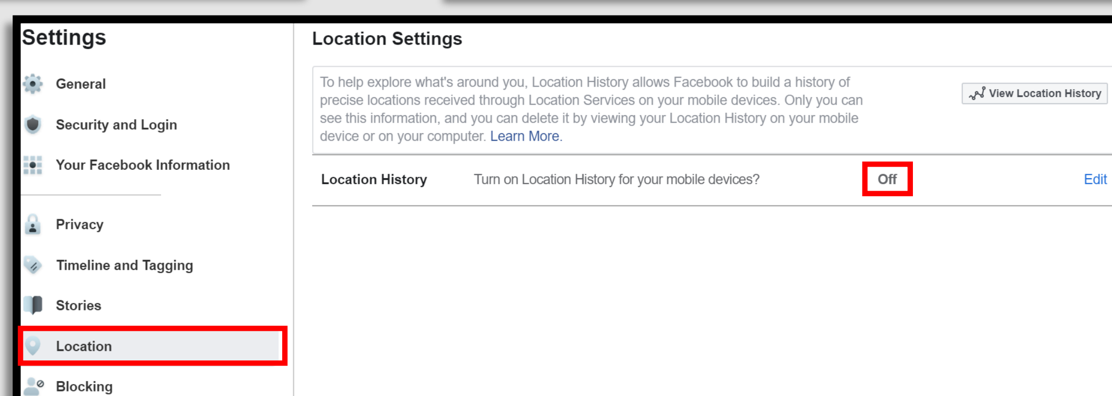
Next, back under "Settings", right under "Privacy", you will find "Timeline and Tagging". Take a few moments here to make sure you agree with all the settings. Some recommendations for this section are the following: ensure nothing is set to "Public"; make sure to turn "On" each section under "Review" so that no one can tag you in anything without your permission.

Under "Review", you can also view your profile from the perspective of the public, or people who are not your "Friends". Simply select "View As". While reviewing your profile from the public perspective, take note of anything you see that you might want to lock down later, such as old profile pictures.



Since the "Stories" function has become more popular, it is important to remember it also needs to be locked down. Facebook has created a new feature that prohibits others from sharing your "Stories". Select "Stories" from the "Settings" menu, and set both "Sharing Options" to "Don't Allow".



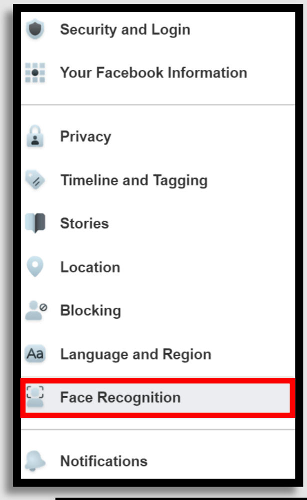


In the "Location" section make sure Facebook shows your location is "Off". You must also turn your location settings to "Off" on each of your mobile devices to ensure the pictures/data you post do not contain geolocation information.

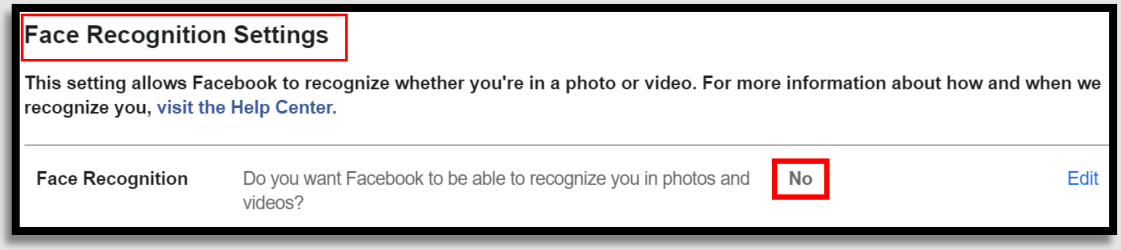
Letting people know where you are at the exact moment you are there can be an extremely dangerous choice. #thinkbeforeyoupost

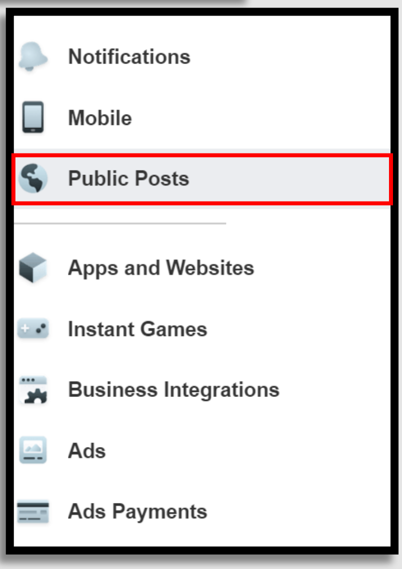
FACEBOOK SMART CARD

Personal Computer (PC) Version

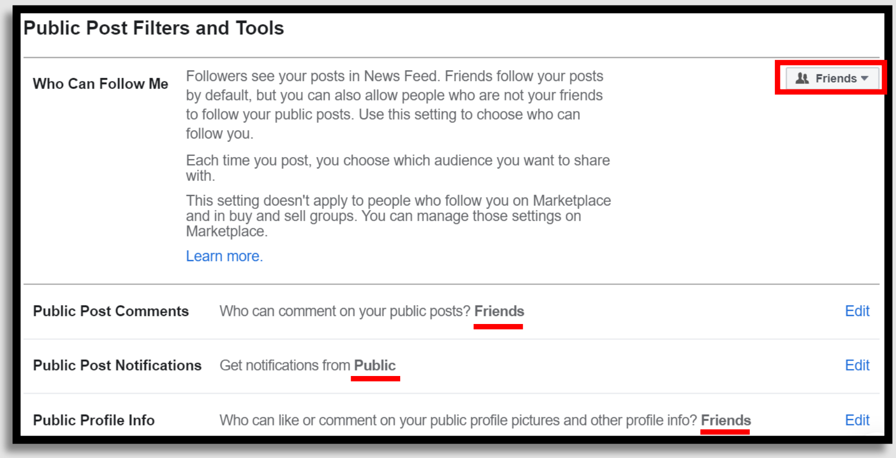


Do you want Facebook to be able to recognize your face in pictures? Neither do we! Recommended setting for this section is easy — "No".

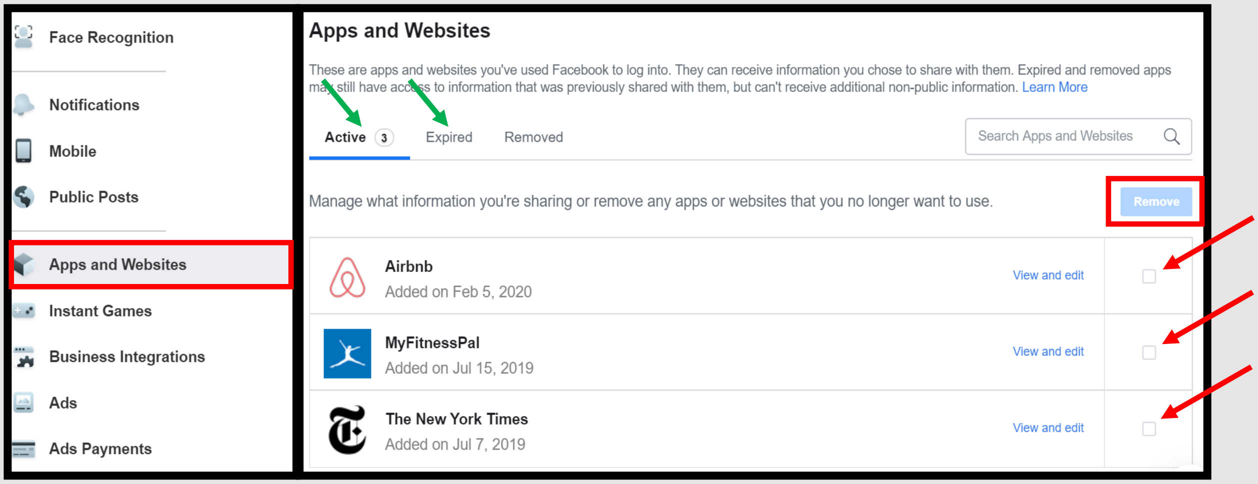




Next, in the "Public Post Filters and Tools" section, under "Public Posts" in "Settings" let's review public filtering. It is recommended that you do not let the "Public" follow you. Remember, allowing the "Public" to follow you means anyone with a Facebook profile, and possibly even without one, can see what you are posting.



Now let's clean up all the "Apps and Websites" that Facebook has been allowing to use your information. Here you can review all the applications you may have allowed access to your Facebook account. Select "Apps and Websites", in the "Settings" menu.

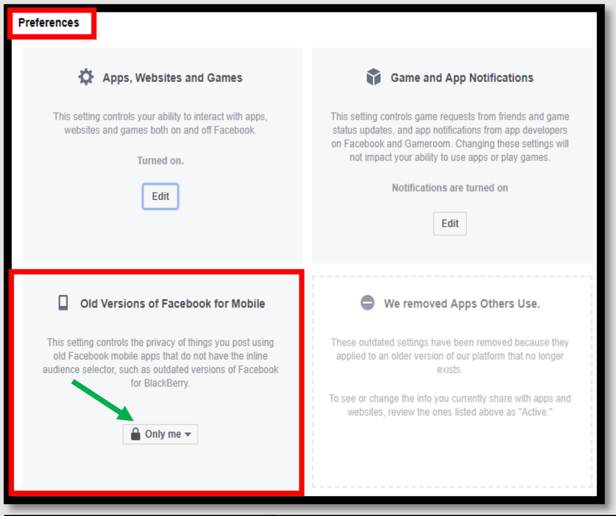


If you find apps that you no longer wish to have access, simply check the box and then select "Remove". Make sure to do this for the "Active" and "Expired" sections tabs at the top of this box.

Managing your Facebook Profile is important. Equally as important, is knowing what other users are saying about you. #ownyourprofile #fbtagging

FACEBOOK SMART CARD

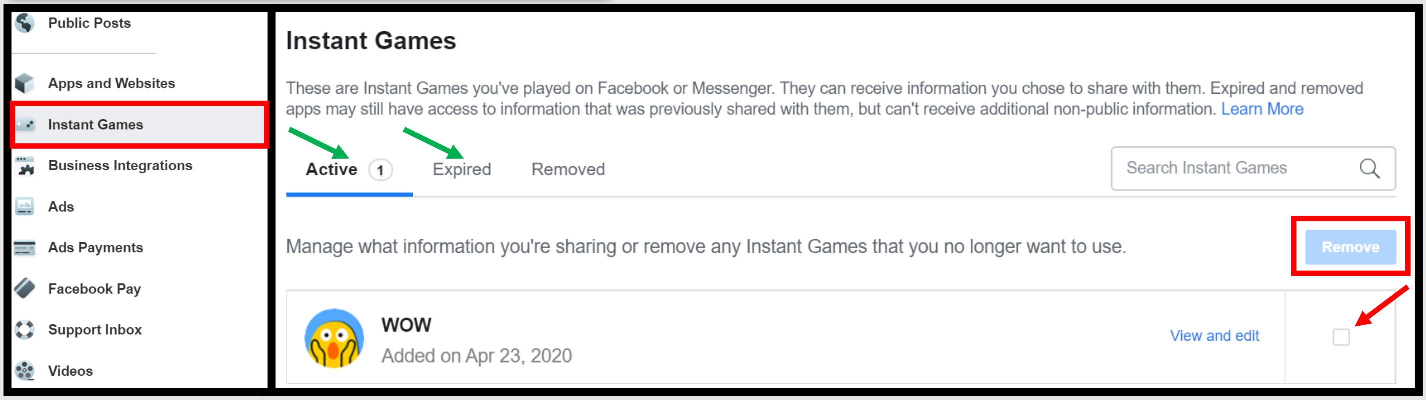
Personal Computer (PC) Version

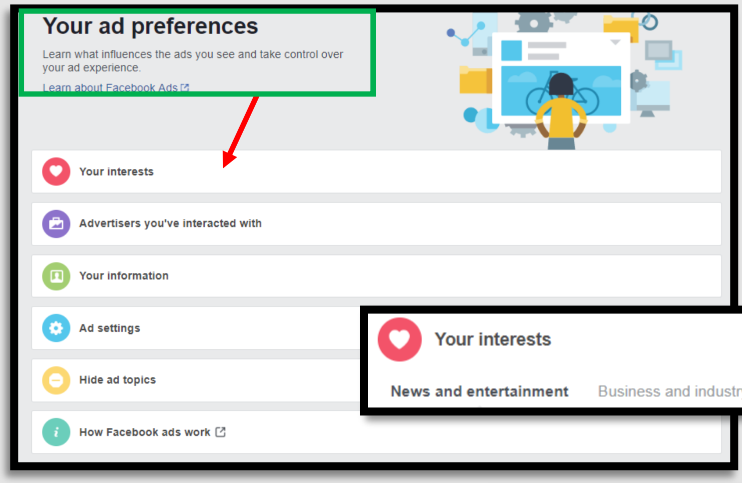


Next scroll down to the "Preferences" section on the same page. Here you can control how "Apps, Websites, and Games" are able to interact with your Facebook account.

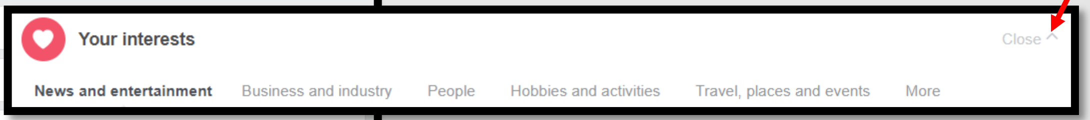
We recommend that you keep the "Old Version of Facebook for Mobile" in a setting set to "Only Me" so that it is not viewable to any one else.

Now click on the "Instant Games" tab in the "Settings" menu. Review any games you may have allowed access to your account, the type of data they are collecting, and whether or not you want them to remain. If you choose to, you can delete any of the games, much like you just did in the "Apps and Websites" section. (see below)





Let's look at "Your ad preferences". Select "Ads" on the "Settings" menu (not shown), and see the page "Your ads preferences". Under each tab you can review your information by clicking on the down arrow in the right hand corner of each category. Under "Your Interest" and "Advertisers you've interacted with", you can remove any of the selections by clicking the "x" at the right of each tile.



> *Some users are so overwhelmed by the curiosity that they tend to ignore some of the risks involved, and inadvertently give the app access to sensitive data.*[1]

References:

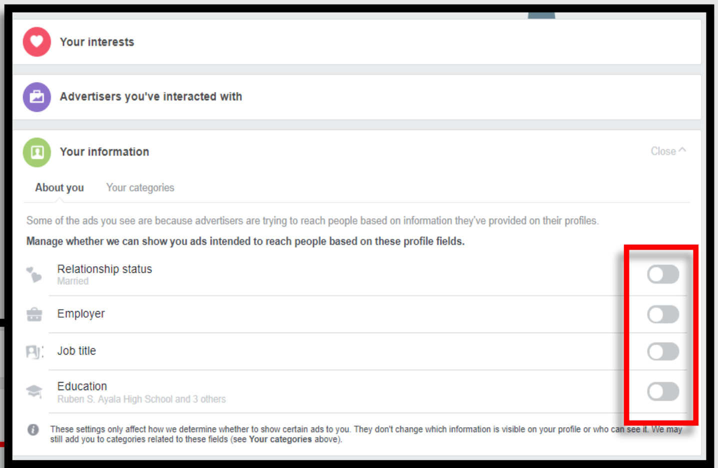
1. https://www.thequint.com/tech-and-auto/tech-news/sharing-data-with-facebook-apps-and-games-can-have-serious-consequences

Never give up too much information, drawing out your family members on Facebook could help an Identity Thief answer security questions about you. #themoreyouknow

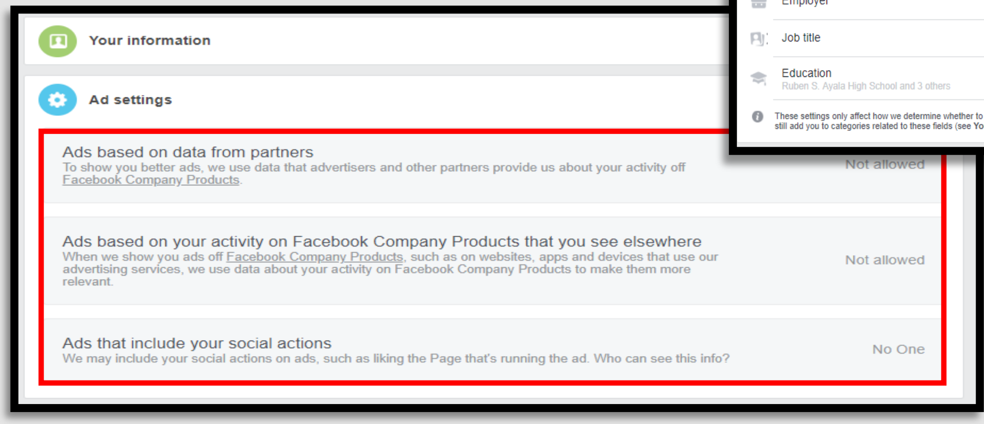
FACEBOOK SMART CARD

Personal Computer (PC) Version

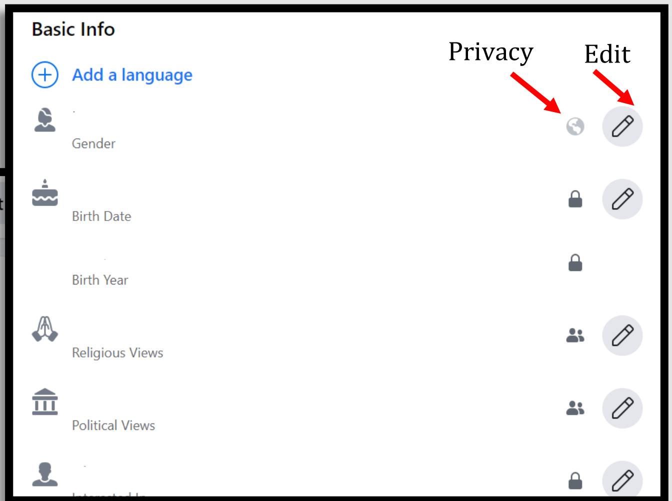
Under the "Your Information" tab, ensure all the sliders are off (greyed out) so that none of your information is provided by Facebook to advertisers. It is important to limit the information advertisers have access to about you. This will help to ensure your information doesn't show up on advertisements and will limit unwanted ads on your timeline.

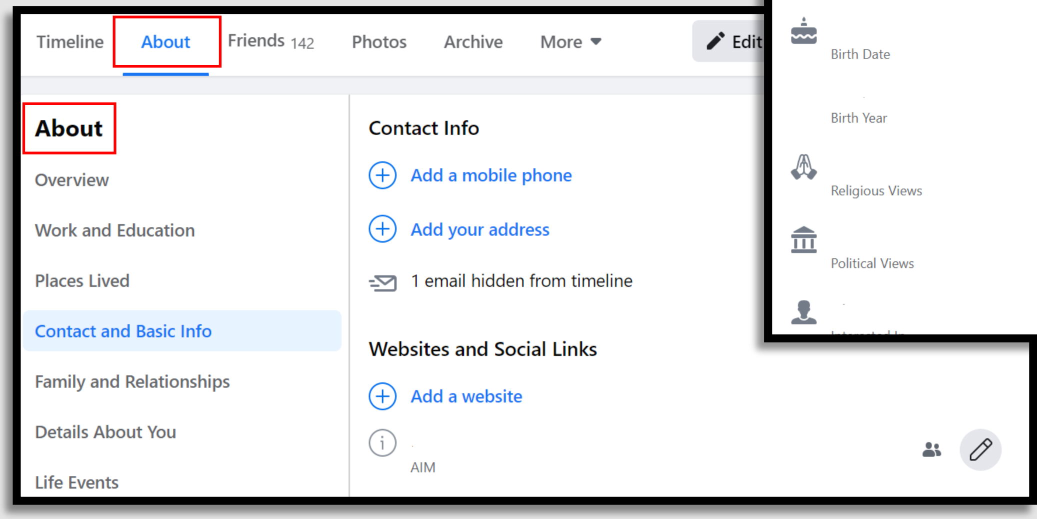


Under "Ad Settings", it is recommended that you select "Not Allowed" or "No One" for each category.



Now that you have completed the "Settings" sections, let's move on to secure your personal profile information. First, from the "Home" screen, select your "Profile Picture" or "Username". Next, select "About" on your personal "Profile Page". You should go through each selection in the "About" section and make sure the privacy settings are as secure as possible. You will see 2 update opportunities for each item: 1) privacy, and 2) edit. We recommend you choose "Only Me" as much as possible, and "Friends" as a second choice for who each piece of information is presented to. When "editing", remember to include the least amount of information possible — wherever you can, leave your inputs blank, and where you provide information, keep it vague.

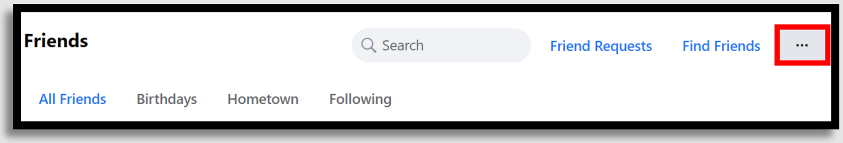


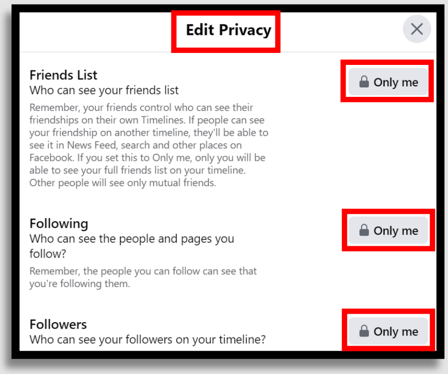


How much information does a criminal have to have to make you think you know them and can therefore trust them? #lockitdown

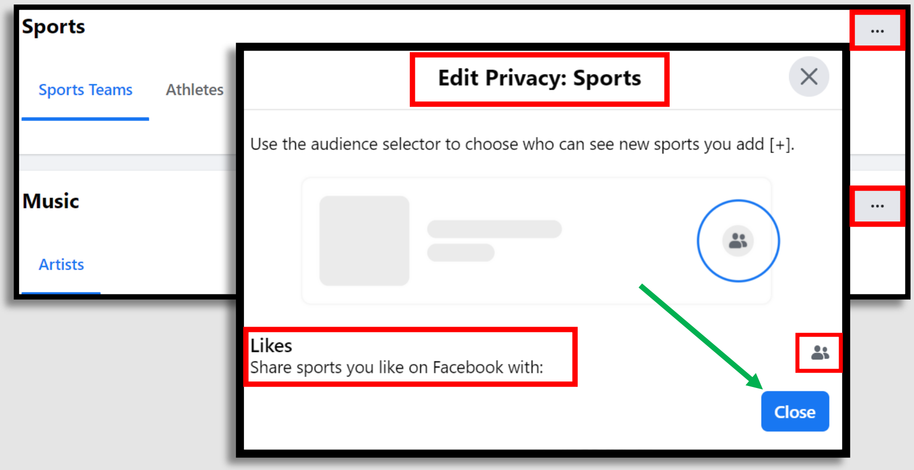
FACEBOOK SMART CARD

Personal Computer (PC) Version

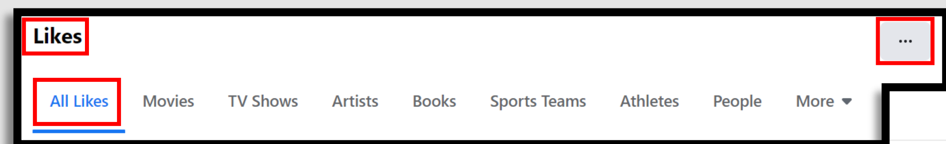


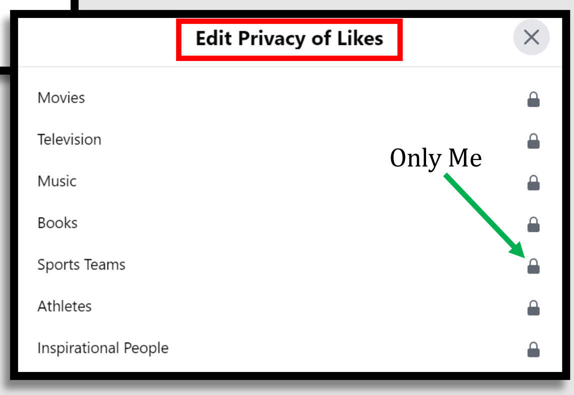


Below this, see your "Friends" section. Here, select the "Options", or " . . . " button in the upper right corner of the section. Select "Edit Privacy" (not shown, but only option), then adjust the settings in the pop-up box (see right). We recommend setting all three options to "Only Me".



The things you "Like" on Facebook can be analyzed in order to create a pretty accurate profile of you. This information can be a lot more dangerous than you might imagine. In the "About" section, you can control who sees your "Likes" by selecting the "…" button to the right of each interest category (eg: sports, music), then select "Edit Privacy", and set your "Likes Privacy" icon to "Only Me" or "Friends" on each section. "Only Me" is the most secure choice, and recommended whenever possible.





Although you have enhanced the security of your "Likes" above, you will need to repeat the process in one additional section. Beneath all the categories of your interests on your "About" page (under "Books"), you will see a "Likes" section. You will want to control the presentation of "Likes" here as well. Select the "…" button, then "Edit the privacy of your likes", then select "Only Me" on each category.

Think
once before you act
twice before you speak
and three times
before you post
on Facebook

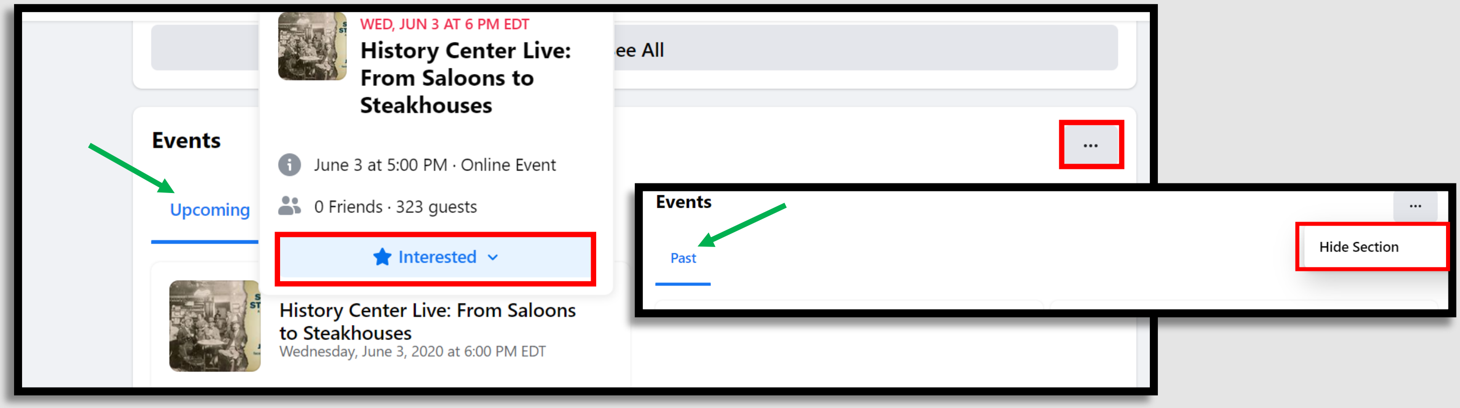
*Social Engineers or Human Hackers are more likely to convince you that they know you if they have access to personal information about you. This information can be in the form of your likes/hobbies, friends, events you will or have been to or what schools you have previously attended. They can even review past posts you may have open to the public for some additional insight. Once they have convinced you that you are "old friends" there is significant danger. They could convince you to meet in person, lend them money, steal your identity, or get close to your children. The best defense is to limit who can see this information about you to "Only Me" or "Friends".

How many "Friends" do you have on Facebook? Would you recognize them if they were standing right in front of you? #FBpurge #whoareyourfbfriends

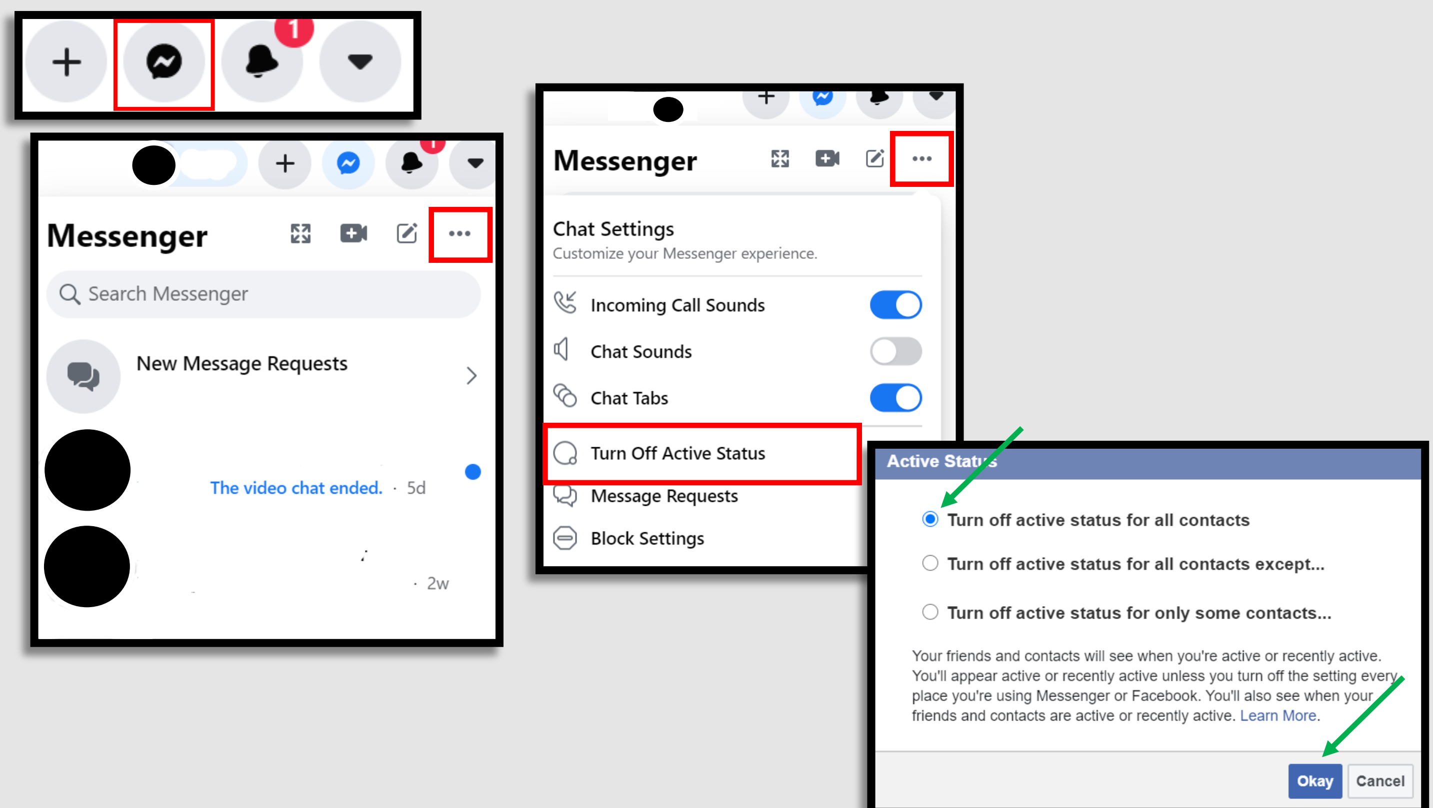
FACEBOOK SMART CARD

Personal Computer (PC) Version

Next, as you continue to scroll down the page, you may want to go through all your “Events” to see if there are any you can delete. Also, make sure all your events are set to “Only Me” by hovering over the event title, clicking the “Going” button, and looking to the bottom line of the pop-up for “Visible to the Hosts and Only Me” (not shown). If you have an upcoming “Event” or an “Event” that you are “interested in” that is not set to “Only Me”, be aware that anyone will be able to see that you will be attending that event. You also have the option of hiding the entire ‘Events” section. Go to the “ . . . “ button at the top right corner of the “Events” section, select “Hide Section”. This is the quickest and easiest way to secure this information, and is what we recommend. Remember to do this in both “Upcoming” and “Past” sections. (see arrows above)



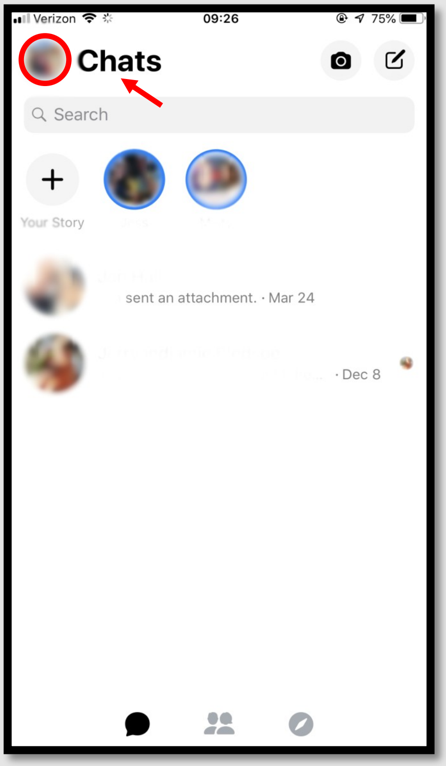
Next is the “Messenger” feature, there are a few things to cover in order to protect your privacy here. First, go to the top of the page to the “Messenger” icon, and see the “Messenger” dropdown menu. Here you will be able to turn “On” and “Off” your “Status” on “Messenger”. Select the “. . . “ button, then select “Turn Off Active Status”. Choose one of the three options on the pop-up screen, and select “Okay”. In this way, you can control who, if anyone, can see that you are actively using Facebook at any given time.

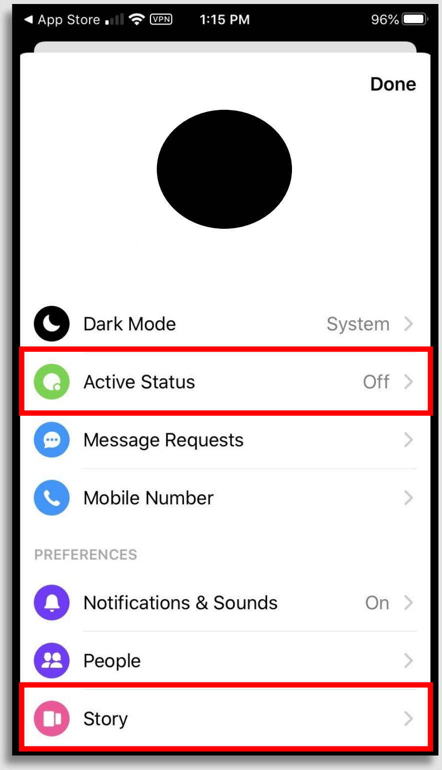


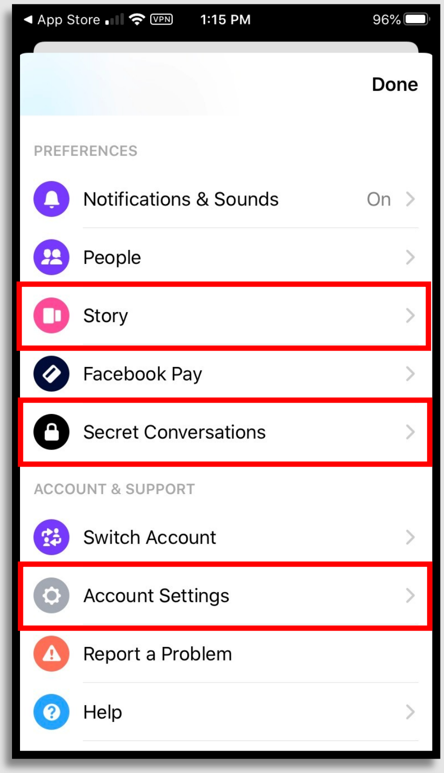
How many “Friends” do you have on Facebook? Would you recognize them if they were standing right in front of you? #FBpurge #whoareyourfbfriends

FACEBOOK SMART CARD

Mobile Device Version



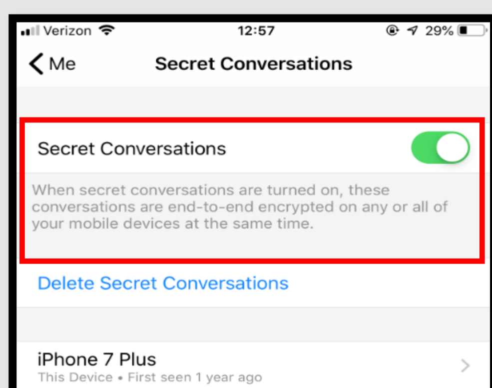




The final feature you may want to review your "Messenger" app, and this information may mainly apply to your mobile device. Facebook has launched a dedicated website interface, and separated its messaging functionality from the main Facebook app, allowing users to use the web interface or download one of the stand-alone apps. What this means for you is that you may be taken outside of Facebook sometimes, when you are trying to access Facebook "Messenger". Also, your computer version of "Messenger" may look different from your mobile device version, and may he have more or less features. This page addresses Facebook "Messenger" on mobile device.

Once logged into Facebook "Messenger", head to the top left of the screen, select your "Profile Picture" (highlighted above in red). Here you can review all of the additional settings "Messenger" has to offer. You can chose whether or not you want people to know when you are "Active" on "Messenger" by selecting the "Active Status" and turning it "Off." You can also set your "Story" accesses the way you want—we recommend setting to "Custom", by which you can select your audience manually, or "Friends". You can also review your "Account Settings" (eg: personal info, privacy, ads).

Finally, Facebook "Messenger" has a feature called "Secret Conversations" where your conversations are encrypted end-to-end. To turn this feature "On", select your "Profile Picture", select "Secret Conversations" where you will then be able to turn the feature on. If you have children that use Facebook Messenger it is important to know about this feature so you can monitor it as you see fit.

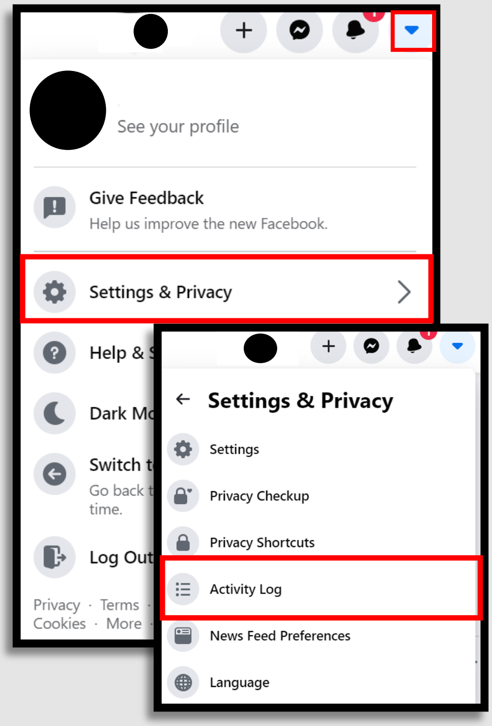


Remember, it is important to lock down your Facebook Messenger the same way you lock down the rest of your Facebook.

FACEBOOK SMART CARD

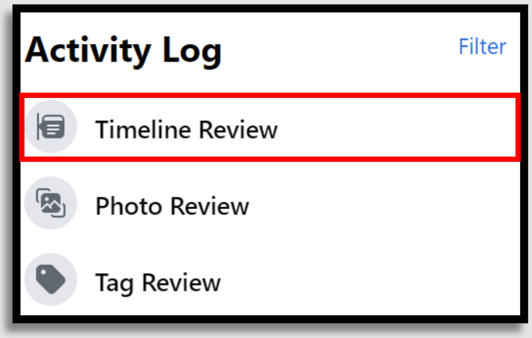
Personal Computer (PC) Version

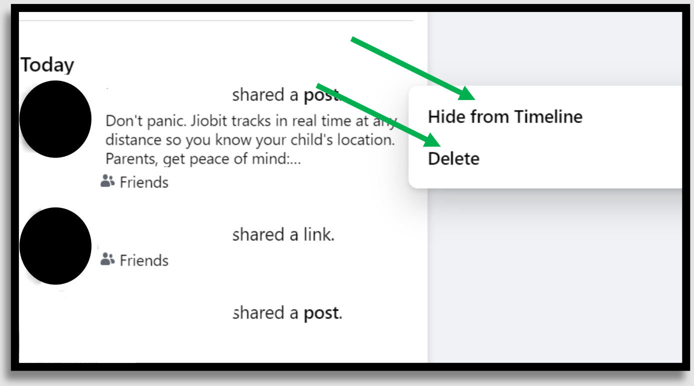
Finally, lets go back to Facebook's "Activity Log", accessed from the "Settings & Privacy" option under the "Down Arrow" in the right upper corner of the "Home Page". The "Activity Log" allows you to review any click of the button (photos, comments, Likes, posts, etc.) or tag that has ever occurred and been associated with your profile. This is the central location for cleaning up your Facebook profile.



More specifically, from the "Activity Log" you can review information by date, all the way from the creation of the profile to the present. You can also see if a post is viewable to the public or just to friends, as well as review any posts you have been "Tagged" in. Finally, the "Activity Log" allows you to remove any actions you have taken on Facebook as well as any "Tags" that someone else may have posted.

From the "Activity Log" page, select "Timeline Review" first. A list of "Filters" appears, and you can go through each one. You can go through each post, photo and tag on your account, and hide or delete them as you decide.





Just select the "… " button that you will see when you hover to the right of the post, and select "Hide from Timeline" or "Delete". Alternatively, you can click on the post and it will open in the box to the right of the page, where you can select the "… " button and choose from several additional options, including "Edit post" and "Edit audience".

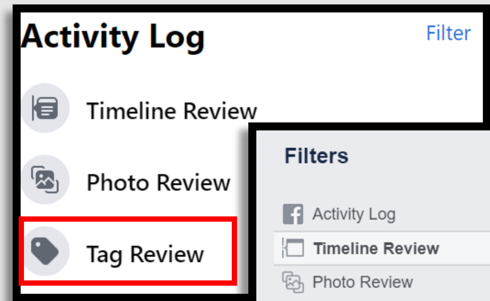
You can limit each post's visibility by setting every one to "Only Me" or "Friends". Remember if you "Like" or "Comment" on someone's post whose privacy settings are set to "Public", your comment will also be "Public". You can only set your own privacy settings for your profile, and once you reach outside of your profile, you have no control over privacy.

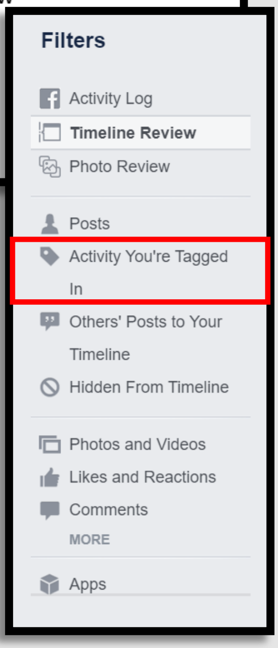
Correcting posts might be tempting, but think about what correcting that post says about you and the information you have access to. #staysafeonfb

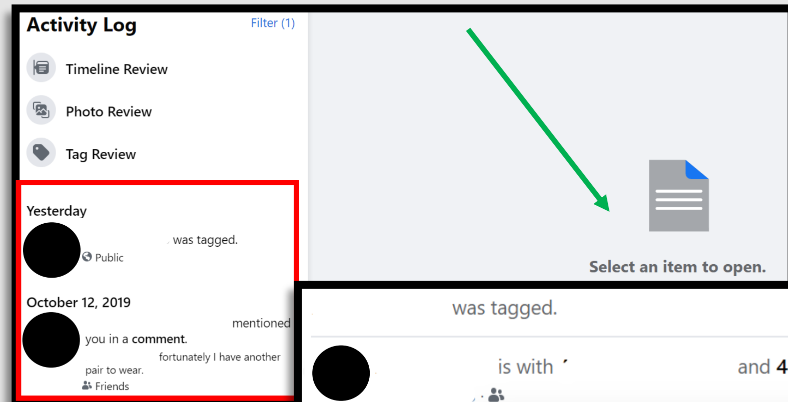
FACEBOOK SMART CARD

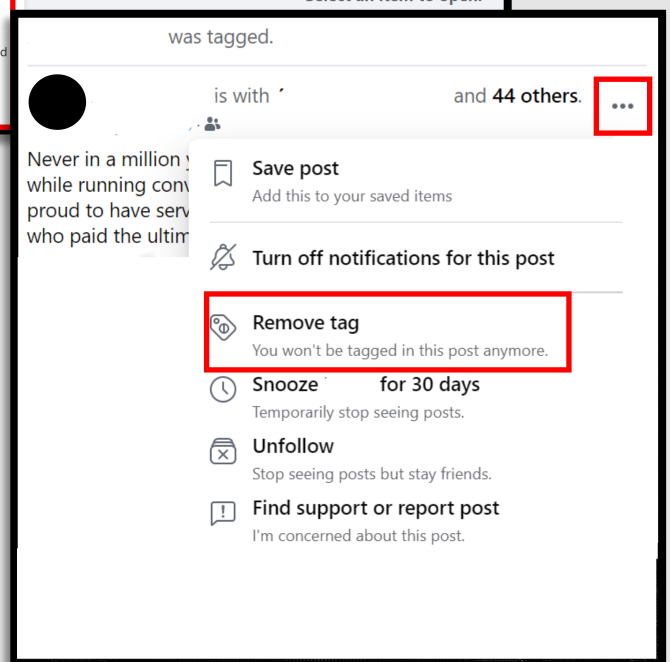
Personal Computer (PC) Version

Finally, let's address "Tags", which are a feature of Facebook by which other people can call attention to your name by "Tagging" a photo that you may or may not be in, or "Mentioning" you in a "Post" or "Comment". People can do this without your permission if you don't have the "Tagging" options selected as we have done in this Card. When you are "Tagged" in a photo, that photo is viewable by the "Public", while also drawing attention to your name. Here is what you can do about it.









First, in "Activity Log", select "Tag Review", then select "Activity You're Tagged In". All the "Posts", "Comments", and photos you are tagged in appear in the left column. Select the "Post" you want to view and "Untag". The post will open in the box to the right of the screen. Select the " . . . " in the right upper corner of the post, and select "Remove Tag" on the drop-down.

Note: If you remove a "Tag" of yourself, it will NOT notify the individual who owns the post/picture that you have removed the tag.

Remember: Although the photo is "Untagged" and no longer on your profile, the photo has ***not*** been deleted from Facebook. It will remain on the profile of the individual who originally posted the photo. *Backdoor avenues* used in finding your profile may still exist (e.g. via a tagged photo of you on your spouse's profile or simply finding your name in the comments of the picture/post).

If you'd like for the photo to be removed, the best way is to ask the individual to delete the photo/post.

I think it is important to fortify ourselves online the same way we would fortify our homes if we knew we were under attack.

-II MEF Commanding General LtGen Hedelund's response when asked for his take on social media and force protection.

Don't think you can hide your FB profile by using a different name. Better to assume people can find you and set your privacy/security settings accordingly. #bettersafethansorry

FACEBOOK SMART CARD

Indicators of Possible Account Compromise:

Do you think your account may have been compromised or hacked? Have you noticed any of the following:

* Unexpected posts posted by your account
* Any Direct Messages sent from your account that you did not initiate
* Other account behaviors you didn't perform or approve (like following, unfollowing, blocking, etc.)
* A notification from Facebook stating that your account may be compromised
* A notification from Facebook stating that your account information (bio, name, etc.) has changed
* Your password is no longer working or you are being prompted to reset it. *If this occurs it is highly recommended that you sign-in online and change your password immediately.

If you said "Yes" to any of the above , it is advised you take the following actions:

- Delete any unwanted posts that were posted while your account was compromised
- Scan your computers for viruses and malware, especially if unauthorized account behaviors continue to be posted after you've changed your password
- Make sure to change your password. Always use a strong password you haven't used elsewhere and would be difficult to guess
- Consider using login verification (if you haven't done so already), instead of relying on just a password. Login verification introduces a second check to make sure that you and only you can access your Facebook account
- Be sure to check that your email is secure. It may be worth changing the password to both your Facebook account and the email associated with your Facebook account. *If you feel your email may have been compromised and need help finding the right contact information for your email provider please see page 21 of this smart book under the "blue box" at the bottom of the page.

If you need to report **Spam/Harassment**: Go to https://www.facebook.com/help/968185709965912/?helpref=hc_fnav

If your account was hacked: https://www.facebook.com/help/hacked

Also, if you find that someone is impersonating you Facebook: https://www.facebook.com/help/hacked then scroll down to the "Impersonation Accounts" section and follow the directions. If you do not have a Facebook account and want to report an impersonating account go to: https://www.facebook.com/help/contact/295309487309948

To find additional "Security Features and Tips go to: https://www.facebook.com/help/379220725465972?helpref=faq_content

If you still need help or have questions, you can always contact Facebook by: https://www.facebook.com/facebookapp where you can message a Bot Facebook created to help answer questions while they work on building a live customer support capability.

If someone is threatening to share information (ex: messages or photos) on Facebook of your child that they do not want shared you should report it to the local law enforcement. Facebook also says you can do the following: Report the incident to Facebook https://www.facebook.com/help/contact/567360146613371, then make sure that this person is blocked so they no longer have access to your child. It is important to talk to your children about this possibility before they begin to use social media so that they know what to do should this happen to them.